SHUB & JOHNS LLC
Jonathan Shub (No. 237708)
Benjamin F. Johns
Samantha E. Holbrook
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
(610) 477-8380
jshub@shublawyers.com
bjohns@shublawyers.com
sholbrook@shublawyers.com

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

MATTHEW RUTLEDGE, individually and on behalf of all others similarly situated, Plaintiff, v. KEENAN & ASSOCIATES, Defendant.	Case No.: 5:24-cv-0263 CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Matthew Rutledge ("Plaintiff" or "Rutledge"), individually and on behalf of all others similarly situated, brings this Class Action Complaint and alleges the following against Defendant Keenan & Associates ("Keenan" or "Defendant"), based upon personal knowledge with respect to himself and upon information and belief derived from, among other things, investigation of counsel

and review of public documents as to all other matters:

NATURE OF THE ACTION

1. This class action arises out of the recent data breach (the "Data Breach") involving Keenan, which collected and stored certain personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information") of the Plaintiff and the putative Class Members.

2. According to Keenan, the PII and PHI compromised in the Data Breach included highly-sensitive information including dates of birth, Social Security numbers, passport numbers, driver's license numbers, health insurance information, and other general health information.[1]

3. Social Security numbers are particularly valuable to criminals. This information can be sold and traded on the dark web black market. The compromise of a Social Security number is particularly troubling because it cannot be easily changed and can be misused in a range of nefarious activities, such as filing fraudulent tax returns to steal tax refund payments, opening new accounts to take out loans, and other forms of identity theft.

4. The Data Breach was a direct result of Keenan's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to

[1] Sample Keenan *Notice of Data Security Incident*, available at https://oag.ca.gov/system/files/EXPERIAN_K7150_KeenanAssociates_Notice%20Letter_Redacted.pdf (last accessed Feb. 2, 2024) (hereinafter, "Notice").

protect consumers' Private Information. Keenan has acknowledged that the cybersecurity attack occurred "at various times between August 21, 2023 and August 27, 2023," but that it waited until January 26, 2024 to begin contacting Class Members. *Id.*

5. According to a notice of data breach filed with the Attorney General of Maine, the Data Breach has affected 1,509,616 individuals.[2]

6. This was not a passive data breach where, for example, it is unclear whether the compromised data was targeted or even seen. By Keenan's own acknowledgement, the data breach here occurred because an "unauthorized third party" was able to "gain[] access to" and "obtain[]" data from Keenan's internal computer systems.[3]

7. Plaintiff brings this lawsuit on behalf of himself and all of those similarly situated to address Keenan's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information was unsecured and left open to the unauthorized access of any unknown third party.

---

[2] https://apps.web.maine.gov/online/aeviewer/ME/40/21846091-dc71-4ecc-9db8-a3be3e84a7d0.shtml (last accessed Feb. 2, 2024).

[3] *Id.*

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because: (i) the amount in controversy exceeds $5 million, exclusive of interest and costs; (ii) the number of class members exceeds 100 and (iii) minimal diversity exists because many class members, including Plaintiff Rutledge has different citizenship from Defendant. This Court has personal jurisdiction over Defendant because it operates and is headquartered in this District and conducts substantial business in this District.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiffs and Class Members in this District.

PARTIES

Plaintiffs

10. Plaintiff Matthew Rutledge is an adult, who at all relevant times, was a resident and citizen of San Bernardino County in the state of California.

11. Based on his comprehensive and recent relationship with Keenan, Plaintiff Rutledge has a good faith belief that his Private Information was compromised in the Data Breach that occurred on or around August 21, 2023.

12. Beginning right around the time the Data Breach occurred in August

2023, Plaintiff Rutledge began to receive notifications that someone had made login attempts and attempted to change his passwords for his existing accounts with credit reporting agencies, online survey websites, and his personal email account. He also received notifications from companies who pulled his credit report despite the fact that he never made any requests or engaged in transactions that would merit pulling his credit report.

13. Plaintiff Rutledge has spent several hours addressing the unauthorized activity and otherwise monitoring his accounts as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Rutledge otherwise would have spent on other activities, such as work and/or recreation.

14. Plaintiff Rutledge plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

Defendant

15. Defendant Keenan & Associates is an insurance consulting and brokerage firm who services schools, public agencies, and health care organizations.[4] Its principal place of business and headquarters is located at 2355

[4] *See About Keenan*, KEENAN https://www.keenan.com/About (last visited Feb. 2, 2024).

Crenshaw Blvd., Suite 200, Torrance, California 90501.[5]

FACTUAL ALLEGATIONS

16. Keenan sells employee benefits, workers compensation coverage, and property & liability coverage to California educational institutions, public agencies and health care organizations.[6]

17. Due to the nature of the services Keenan provides, it receives and is entrusted with securely storing consumers' Private Information, which includes, *inter alia*, individuals' full name, date of birth, Social Security number, passport number, driver's license number, health insurance information, and general health information.

Keenan's Unsecure Data Management and Disclosure of Data Breach

18. Plaintiff and Class Members provided their Private Information to Keenan with the reasonable expectation and mutual understanding that Keenan would comply with its obligations to keep such information confidential and secure from unauthorized access.

19. Data security is purportedly a critical component of Keenan's business model. On a section of its website entitled "Privacy Policy," Keenan makes the

[5] https://apps.web.maine.gov/online/aeviewer/ME/40/21846091-dc71-4ecc-9db8-a3be3e84a7d0.shtml (last accessed Feb. 2, 2024).

[6] https://www.keenan.com/Solutions (last visited Feb. 2, 2024).

following statements:[7]

- Keenan & Associates (including our affiliates and subsidiaries) ("Keenan", "we", "us" or "our") respects your privacy and takes our privacy responsibility very seriously and **is committed to protecting it in a manner consistent with applicable law** and this statement.

- This Policy and notice applies to your Personal Information that we may collect, use, receive, and disclose and describes our practices for collecting, using, maintaining, protecting and disclosing that information in the course of providing our services.

  . . .

- **We have implemented measures reasonably designed to protect and secure your Personal Information from** accidental loss, misuse, and from **unauthorized access, use, alteration, and disclosure**.

20. Keenan also maintains a "California Privacy Policy", which contains information concerning the requirements of California Consumer Privacy Act ("CCPA") as it relates to the storage of the data of California residents.[8] A section of the California Privacy Policy, under the header "Why We Collect Personal Information and How We Use It," delineates the various circumstances under which Keenan may share PII and PHI for legitimate business purposes. It does not include providing that date to "unauthorized third parties"; to the contrary, the Policy states that "[w]e may disclose your personal information to a third party for a business or

[7] https://www.keenan.com/Privacy-Statement (last visited Feb. 2, 2024) (all emphasis supplied).

[8] https://www.keenan.com/CCPA (last visited Feb. 2, 2024).

legal purpose" and "[w]e do not sell your personal information to third parties."[9]

21. Contrary were Keenan's various express assurances that it would take reasonable measures to safeguard the sensitive information entrusted to it – and only share it for an express authorized persons – an "unauthorized" person or persons was able to access its network servers.

22. According to its January 26, 2024 Notice letter concerning the breach, on August 27, 2023, Keenan "noticed disruptions occurring on some Keenan network servers" and "immediately began an investigation and engaged leading third-party cyber security and forensic experts to assist." It later determined that a "an unauthorized party gained access to certain Keenan internal systems at various times between approximately August 21, 2023 and August 27, 2023, and that the unauthorized party obtained some data from Keenan systems."

23. The database files that were compromised included names, mailing addresses, Social Security numbers, personal health information, and other information related to prior productions.

24. To date, Keenan has not disclosed specifics of the attack, such as whether ransomware has been used. It has only told the Maine AG's Office that the breach was an "[e]xternal system breach (hacking)."

25. As such, Keenan failed to secure the PII and PHI of the individuals that

[9] *Id.*

provided it with this sensitive information. It failed to take appropriate steps to protect the PII and PHI of Plaintiff and other Class Members from being disclosed.

Keenan is a HIPAA Covered Entity

26. As a regular and necessary part of its business, Keenan collects and custodies the highly sensitive Private Information of its clients' employees. Indeed, the Data Breach notice states that "health insurance information" and "general health information" were among the types of information compromised in the breach. Keenan is, therefore, required under federal and state law to maintain the strictest confidentiality of the patient's Private Information that it requires, receives, and collects, and Keenan is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

27. Indeed, Keenan's Privacy Policy acknowledges that "[s]ome of the categories of Personal Information that we may collect are special categories of information protected by federal law including your health records (such as your medical history and reports on medical diagnoses, injuries, and treatment)…".[10]

28. As a HIPAA covered entity, Keenan is required to ensure that it will implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including

[10] *See* https://www.keenan.com/Privacy-Statement (last accessed Feb. 2, 2024).

incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

29. Due to the nature of Keenan's business, which includes providing group health insurance to employers, Keenan would be unable to engage in its regular business activities without collecting and aggregating Private Information that it knows and understands to be sensitive and confidential.

30. Plaintiffs and the Class Members relied on Keenan to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information. Plaintiffs and Class Members reasonably expected that Keenan would safeguard their highly sensitive information and keep their Private Information confidential.

31. As described throughout this Complaint, Keenan did not reasonably protect, secure, or store Plaintiffs' and the Class's Sensitive Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information Keenan maintained. Consequently, Keenan allowed for the exfiltration of Plaintiff and Class Members' Private Information.

Keenan Failed to Comply with FTC Guidelines

32. Keenan was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

33. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

34. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[11] The guidelines also recommend that businesses use an intrusion

[11] *See* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Feb. 2, 2024).

detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. *Id.*

35. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

36. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

37. These FTC enforcement actions include actions against healthcare providers and partners like Keenan. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were

unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

38. Keenan failed to properly implement basic data security practices.

39. Keenan's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

40. Keenan was at all times fully aware of the obligation to protect the Private Information of customers and patients. Keenan was also aware of the significant repercussions that would result from its failure to do so.

Keenan Violated its HIPAA Obligations to Safeguard the Private Information

41. Keenan is a covered entity under HIPAA as a business associate (45 C.F.R. § 160.103) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

42. Keenan is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[12] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

43. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

44. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

45. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

a. HIPAA's Security Rule requires Keenan to do the following:

b. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

c. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

[12] *See* https://www.hipaajournal.com/relationship-between-hitech-hipaa-electronic-health-medical-records/ (last accessed Feb. 2, 2024).

d. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

e. Ensure compliance by its workforce.

46. HIPAA also requires Keenan to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Keenan is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

47. HIPAA and HITECH also obligated Keenan to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

48. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Keenan to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery

of the breach."[13]

49. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

50. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

51. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human

---

[13] *See* Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last accessed Feb. 2, 2024).

Services, Security Rule Guidance Material.[14] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[15]

52. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Keenan left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

53. A Data Breach such as the one Keenan experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which

---

[14] *See* https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last accessed Feb. 2, 2024).

[15] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last accessed Feb. 2, 2024).

compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40

54. The Data Breach resulted from a combination of insufficiencies that demonstrate Keenan failed to comply with safeguards mandated by HIPAA regulations.

Plaintiff and the Class Have Suffered Injury as a Result of Keenan's Data Mismanagement

55. As a result of Keenan's failure to implement and follow even the most basic security procedures, Plaintiff's and Class Members' PII and PHI has been and is now in the hands of an unauthorized third-party which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals. Plaintiff and other Class Members now face an increased risk of identity theft, particularly due to the dissemination of their Social Security Number, and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to Keenan's Data Breach.

56. Plaintiff and other Class Members have had their most personal and sensitive Private Information disseminated to the public at large and have experienced and will continue to experience emotional pain and mental anguish and embarrassment.

57. Plaintiff and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those

impacted are under heightened and prolonged anxiety and fear, as they will be at risk for falling victim for cybercrimes for years to come.

58. PII is a valuable property right.[16] The value of PII as a commodity is measurable. "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[17] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[18] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

59. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various

---

[16] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...").

[17] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[18] U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

60. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[19] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[20] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[21]

61. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[22]

62. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived

---

[19] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[20] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

[21] *In the Dark*, VPNOverview.com, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed on Feb. 2, 2024).

[22] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

that consumer of the full monetary value of the consumer's transaction with the company.

63. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[23]

64. Plaintiff and members of the Class, as a whole, must immediately devote time, energy, and money to: 1) closely monitor their bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

65. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse.

---

[23] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Feb. 2, 2024).

For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Keenan's conduct. Further, the value of Plaintiff's and Class Members' Private Information has been diminished by its exposure in the Data Breach.

66. As a result of Keenan's failures, Plaintiff and Class Members are at substantial risk of suffering identity theft and fraud or misuse of their Private Information.

67. Plaintiff and members of the Class suffered actual injury from having PII compromised as a result of Keenan's negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their PII, a form of property that Keenan obtained from Plaintiff; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

68. For the reasons mentioned above, Keenan's conduct, which allowed the Data Breach to occur, caused Plaintiff and members of the Class these significant injuries and harm.

69. Plaintiff brings this class action against Keenan for their failure to properly secure and safeguard Private Information and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their Private Information had been compromised.

70. Plaintiff, individually and on behalf of all other similarly situated individuals, alleges claims in negligence, negligence *per se*, breach of implied contract, breach of fiduciary duty, unjust enrichment, violations of the California Consumer Privacy Act and California Legal Remedies Act, and California's Unfair Competition Law.

CLASS ACTION ALLEGATIONS

71. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated ("the Class"):

Nationwide Class

> All individuals residing in the United States whose Private Information was compromised as a result of the Data Breach, including all individuals who were sent the Notice of the Data Breach on or around January 26, 2024.

In the alternative, Plaintiff seeks to represent the following California class (together with the Nationwide Class, the "Class"):

California Class

> All individuals residing in California whose Private Information was compromised as a result of the Data Breach, including all individuals in California who were sent the Notice of the Data Breach on or around January 26, 2024.

72. Excluded from the Class are Keenan's officers and directors, and any entity in which Keenan has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Keenan. Excluded also from the Class are members of the judiciary to whom this case is assigned, their

families and members of their staff.

73. **Numerosity**: The members of the Class are so numerous that joinder of all of them is impracticable. As noted above, there are approximately 1,509,616 consumers affected.

74. **Existence/Predominance of Common Questions of Fact and Law**: There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Keenan unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII and PHI;

b. Whether Keenan failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Keenan's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Keenan's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Keenan owed a duty to Class Members to safeguard their PII and PHI;

f. Whether Keenan was subject to (and breached) HIPAA, the FTC Act, the California Confidentiality of Medical Information Act and/or the

CCPA;

g. Whether Keenan breached its duty to Class Members to safeguard their PII and PHI;

h. Whether computer hackers obtained Class Members' PII and PHI in the Data Breach;

i. Whether Keenan knew or should have known that its data security systems and monitoring processes were deficient;

j. Whether Keenan's conduct was negligent;

k. Whether Keenan's acts breaching an implied contract they formed with Plaintiff and the Class Members;

l. Whether Keenan was unjustly enriched to the detriment of Plaintiff and the Class;

m. Whether Keenan failed to provide notice of the Data Breach in a timely manner; and

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

75. **Typicality**: Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII and PHI, like that of every other Class Member, was compromised in the Data Breach.

76. **Adequacy**: Plaintiff is an adequate representative for the Class because his interests do not conflict with the interests of the Class that he seeks to

represent. Plaintiff has retained counsel competent and highly experienced in complex class action litigation—including consumer fraud and automobile defect class action cases—and counsel intends to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his experienced counsel.

77. **Superiority**: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and members of the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Keenan's conduct. It would be virtually impossible for members of the Class individually to redress effectively the wrongs done to them by Keenan. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, an economy of scale, and comprehensive supervision by a single court. Upon information and belief, members of the Class can be readily identified and notified based upon, *inter alia*, the records (including databases, e-mails, dealership records and files, etc.) Keenan maintains regarding their consumers.

78. Defendant has acted, and refuses to act, on grounds generally applicable to the Class, thereby making appropriate final equitable relief with respect to the Class as a whole.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff Rutledge and the Nationwide Class or, alternatively, the California Class)

79. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

80. Keenan owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their PII and PHI in its possession, custody, or control.

81. Keenan knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class Members' PII and PHI and the importance of maintaining secure systems. Keenan knew, or should have known, of the vast uptick in data breaches in recent years. Keenan had a duty to protect the PII and PHI of Plaintiff and Class Members.

82. Given the nature of Keenan's business, the sensitivity and value of the PII and PHI it maintains, and the resources at its disposal, Keenan should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which Keenan had a duty to prevent.

83. Keenan breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII and PHI entrusted to it—including Plaintiff's and Class Members' PII and PHI.

84. It was reasonably foreseeable to Keenan that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' PII and PHI to unauthorized individuals.

85. But for Keenan's negligent conduct or breach of the above-described duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

86. As a result of Keenan's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying expenditures for

protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII and PHI; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII and PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiff Rutledge and the Nationwide Class or, alternatively, the California Class)

87. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

88. Keenan's duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Keenan, of failing to employ reasonable measures to protect and secure PII and PHI.

89. Keenan violated Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class Members' PII and PHI and not complying with applicable industry standards. Keenan's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtains

and stores, and the foreseeable consequences of a data breach involving PII and PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

90. Keenan's violations of Security Rules and Section 5 of the FTCA constitutes negligence per se.

91. Plaintiff and Class Members are within the class of persons that Security Rules and Section 5 of the FTCA were intended to protect.

92. The harm occurring as a result of the Data Breach is the type of harm Security Rules and Section 5 of the FTCA were intended to guard against.

93. It was reasonably foreseeable to Keenan that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' PII and PHI to unauthorized individuals.

94. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Keenan's violations of Security Rules and Section 5 of the FTCA. Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks

justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII and PHI; (iii) breach of the confidentiality of their PII and PHI; (iv) deprivation of the value of their PII and PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach; and (vi) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff Rutledge and the Nationwide Class or, alternatively, the California Class)

95. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

96. Plaintiff and Class Members either directly or indirectly gave Keenan their PII and PHI in confidence, believing that Keenan would protect that information. Plaintiff and Class Members would not have provided Keenan with this information had they known it would not be adequately protected. Keenan's acceptance and storage of Plaintiff's and Class Members' PII and PHI created a fiduciary relationship between Keenan and Plaintiff and Class Members. In light of this relationship, Keenan must act primarily for the benefit of its consumers, which includes safeguarding and protecting Plaintiff's and Class Members' PII and PHI.

97. Keenan has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty

by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII and PHI, failing to safeguard the PII and PHI of Plaintiff and Class Members it collected.

98. As a direct and proximate result of Keenan's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII and PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII and PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII and PHI which remains in Keenan's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII and PHI compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff Rutledge and the Nationwide Class or, alternatively, the California Class)

99. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein. This claim is pleaded in the alternative to the implied contract claim pursuant to Fed. R. Civ. P. 8(d).

100. Plaintiff and Class Members conferred a monetary benefit upon

Keenan in the form of monies paid for production services or other services.

101. Keenan accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Keenan also benefitted from the receipt of Plaintiff's and Class Members' PII and PHI.

102. As a result of Keenan's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

103. Keenan should not be permitted to retain the money belonging to Plaintiff and Class Members because Keenan failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards.

104. Keenan should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff Rutledge and the Nationwide Class or, alternatively, the California Class)

105. Plaintiff realleges and incorporates by reference all allegations of the

preceding factual allegations as though fully set forth herein.

106. Defendant required Plaintiff and Class Members to provide, or authorize the transfer of, their PII and PHI in order for Keenan to provide services. In exchange, Keenan entered into implied contracts with Plaintiff and Class Members in which Keenan agreed to comply with its statutory and common law duties to protect Plaintiff's and Class Members' PII and PHI and to timely notify them in the event of a data breach.

107. Plaintiff and Class Members would not have provided their PII and PHI to Keenan had they known that Keenan would not safeguard their PII and PHI, as promised, or provide timely notice of a data breach.

108. Plaintiff and Class Members fully performed their obligations under their implied contracts with Keenan.

109. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII and PHI and by failing to provide them with timely and accurate notice of the Data Breach.

110. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Keenan's breach of its implied contracts with Plaintiff and Class Members.

COUNT VI
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018
Cal. Civ. Code §§ 1798.100 *et seq.* ("CCPA")
(On Behalf of Plaintiff Rutledge and the Nationwide Class or, alternatively, the California Class)

111. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

112. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access.

113. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on certain businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

114. Keenan is subject to the CCPA and failed to implement such procedures which resulted in the Data Breach.

115. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security

procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

116. Plaintiff is a "consumer" as defined by Civ. Code § 1798.140(g) because he is natural person residing in the state of California.

117. Keenan is a "business" as defined by Civ. Code § 1798.140(c).

118. The CCPA provides that "personal information" includes "[a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted . . . (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." *See* Civ. Code § 1798.150(a)(1); Civ. Code § 1798.81.5(d)(1)(A).

119. Plaintiff's Private Information compromised in the Data Breach constitutes "personal information" within the meaning of the CCPA.

120. Through the Data Breach, Plaintiff's private information was accessed without authorization, exfiltrated, and stolen by criminals in a nonencrypted and/or nonredacted format.

121. The Data Breach occurred as a result of Keenan's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

122. Simultaneously herewith, Plaintiff is providing notice to Defendants pursuant to Cal. Civ. Code § 1798.150(b)(1), identifying the specific provisions of the CCPA. Plaintiff alleges Keenan has violated or is violating. Although a cure is not possible under the circumstances, if (as expected) Keenan is unable to cure or does not cure the violation within 30 days, Plaintiff will amend this Complaint to pursue actual or statutory damages as permitted by Cal. Civ. Code § 1798.150(a)(1)(A).

123. As a result of Keenan's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks statutory damages of up to $750 per class member (and no less than $100 per class member), actual damages to the extent they exceed statutory damages, injunctive and declaratory relief, and any other relief as deemed appropriate by the Court.

COUNT VII
VIOLATION OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT
Cal. Civ. Code §§ 1750 et seq. ("CLRA")
(On Behalf of Plaintiff Rutledge and the Nationwide Class or, alternatively, the California Class)

124. Plaintiff realleges and incorporates by reference each and every allegation contained elsewhere in this Complaint as if fully set forth herein.

125. This cause of action is brought pursuant to the California Consumers Legal Remedies Act (the "CLRA"), California Civil Code § 1750, *et seq.* This cause of action does not seek monetary damages at this time but is limited solely to

injunctive relief. Plaintiff will later amend this Complaint to seek damages in accordance with the CLRA after providing Defendants with notice required by California Civil Code § 1782.

126. Plaintiff and Class Members are "consumers," as the term is defined by California Civil Code § 1761(d).

127. Plaintiff, Class Members and Defendants have engaged in "transactions," as that term is defined by California Civil Code § 1761(e).

128. The conduct alleged in this Complaint constitutes unfair methods of competition and unfair and deceptive acts and practices for the purpose of the CLRA, and the conduct undertaken by Defendants was likely to deceive consumers.

129. Cal. Civ. Code § 1770(a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

130. Defendants violated this provision by representing that Defendants took appropriate measures to protect Plaintiff's and the Class Members' PII and PHI. Additionally, Defendants improperly handled, stored, or protected either unencrypted or partially encrypted data.

131. As a result, Plaintiff and the Class Members were induced to provide their PII and PHI to Defendants.

132. As a result of engaging in such conduct, Defendants have violated Civil Code § 1770.

133. Pursuant to Civil Code § 1780(a)(2) and (a)(5), Plaintiff seeks an order of this Court that includes, but is not limited to, an order enjoining Defendants from continuing to engage in unlawful, unfair, or fraudulent business practices or any other act prohibited by law.

134. Plaintiff and the Class Members suffered injuries caused by Defendants' misrepresentations, because they provided their PII and PHI believing that Defendants would adequately protect this information.

135. Plaintiff and Class Members may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

136. The unfair and deceptive acts and practices of Defendants, as described above, present a serious threat to Plaintiff and members of the Class.

COUNT VIII
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. and Prof. Code §§ 17200, *et seq.* ("UCL")
(On Behalf of Plaintiff Rutledge and the Nationwide Class or, alternatively, the California Class)

137. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

138. Plaintiffs brings this claim on behalf of themselves and the Class.

139. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

140. By reason of Defendants' above-described wrongful actions, inaction, and omission, the resulting Data Breach, and the unauthorized disclosure of Plaintiff's and Class members' PII and PHI, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning of the UCL.

141. Defendants' business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers, in that the private and confidential PII and PHI of consumers has been compromised for all to see, use, or otherwise exploit.

142. Defendants' practices were unlawful and in violation of the CCPA and CLRA and Defendants' own privacy policy because Defendants Yahoo failed to take reasonable measures to protect Plaintiff's and Class members' PII and PHI.

143. Defendants' business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the PII and PHI they provide to Defendants will remain private and secure, when in fact it was not private and secure.

144. Plaintiff and Class Members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Defendants' above-described wrongful actions, inaction, and omissions including, *inter alia*, the unauthorized release and disclosure of their PII and PHI.

145. Defendants' above-described wrongful actions, inaction, and

omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Class Members' PII and PHI also constitute "unfair" business acts and practices within the meaning of Cal. Bus. & Prof. Code § 17200 *et seq*., in that Defendants' conduct was substantially injurious to Plaintiff and Class Members, offensive to public policy, immoral, unethical, oppressive and unscrupulous, and the gravity of Defendants' conduct outweighs any alleged benefits attributable to such conduct.

146. But for Defendant's misrepresentations and omissions, Plaintiff and Class Members would not have provided their PII and PHI to Defendants, or would have insisted that their PII and PHI be more securely protected.

147. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff and Class Members' PII and PHI, they have been injured as follows: (1) the loss of the opportunity to control how their PII and PHI is used; (2) the diminution in the value and/or use of their PII and PHI entrusted to Defendants; (3) the increased, imminent risk of fraud and identity theft; (4) the compromise, publication, and/or theft of their PII and PHI; and (5) costs associated with monitoring their PII and PHI, amongst other things.

148. Plaintiff takes upon himself enforcement of the laws violated by Defendants in connection with the reckless and negligent disclosure of PII and PHI. There is a financial burden incurred in pursuing this action and it would be against

the interests of justice to penalize Plaintiff by forcing him to pay attorneys' fees and costs from the recovery in this action. Therefore, an award of attorneys' fees and costs is appropriate under California Code of Civil Procedure § 1021.5.

COUNT IX
VIOLATIONS OF CALIFORNIA'S CONFIDENTIALITY OF MEDICAL INFORMATION ACT, Cal. Civ. Code 56 *et seq.* ("CMIA")
(On Behalf of Plaintiff Rutledge and the Nationwide Class or, alternatively, the California Class)

71. Plaintiff realleges and incorporates by reference every paragraph set forth in this Complaint as if fully set forth herein.

72. Plaintiff brings this count on behalf of himself and the California Class.

73. Keenan is a "Contractor" as defined by Cal. Civ. Code § 56.05(d) and/or a "Provider of Health Care" as expressed in Cal. Civ. Code § 56.06, and is therefore subject to the requirements of the CMIA.

74. Plaintiff and members of the California Class are "Patients" as defined by Cal. Civ. Code § 56.05(k).

75. Plaintiff and California Class Members' Private Information that was subject to the Data Breach included "Medical Information" as defined by Cal. Civ. Code §56.05(j).

76. In violation of Cal. Civ. Code § 56.10(a), Keenan disclosed medical information (including Plaintiffs' Private Information) without first obtaining an authorization. The unauthorized disclosure of Plaintiff's and California Class

Members' Private Information to unauthorized individuals in the Data Breach resulted from the affirmative actions of Keenan, who placed two file directories on a web server that was exposed to the public internet. Disclosing Plaintiff's and California Class Members' Private Information on the internet was an affirmative communicative act by Keenan and a violation of Cal. Civ. Code § 56.10(a). Plaintiff's and California Class Members' Private Information was viewed and accessed by unauthorized individuals as a direct and proximate result of Keenan's violation of Cal. Civ. Code § 56.10(a).

77. In violation of Cal. Civ. Code § 56.101(a), Keenan created, maintained, preserved, stored, abandoned, destroyed, or disposed of medical information (including Plaintiff's and California Class Members' Private Information) in a manner that failed to preserve and breached the confidentiality of the information contained therein. This violation resulted from the affirmative actions of Keenan or its agents who exposed two file servers containing Private Information on the public internet. This disclosure was an affirmative communicative act by Keenan and a violation of Cal. Civ. Code § 56.101(a). Plaintiff's and California Class Members' Private Information was viewed by unauthorized individuals as a direct and proximate result of Keenan's violation of Cal. Civ. Code § 56.101(a).

78. Keenan further violated § 56.101(a) because Keenan negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of

medical information (including Plaintiff's and California Class Members' Private Information). This violation resulted from the affirmative actions of Keenan or its agents who exposed two file servers containing Private Information on the public internet. This disclosure was an affirmative communicative act by Keenan and a violation of Cal. Civ. Code § 56.101(a). Plaintiff's and California Class Members' Private Information was viewed by unauthorized individuals as a direct and proximate result of Keenan's violation of Cal. Civ. Code § 56.101(a).

79. Plaintiff's and California Class Members' Private Information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Cal. Civ. Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

80. In violation of Cal. Civ. Code § 56.101(b)(1)(A), Keenan's electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information (including Plaintiff's and California Class Members' Private Information). This violation resulted from the affirmative actions of Keenan or its agents who exposed two file servers containing Private Information on the public internet. This disclosure was an affirmative communicative act by Keenan and a violation of Cal. Civ. Code § 56.101(b)(1)(A). Plaintiff's and California Class Members' Private Information was viewed by unauthorized individuals as a direct and proximate result of Keenan's violation of Cal. Civ. Code § 56.101(b)(1)(A).

81. In violation of Cal. Civ. Code § 56.101(b)91)(B), Keenan's electronic health record system or electronic medical record system failed to automatically record and preserve any change or deletion of any electronically stored medical information (including Plaintiff Rutledge's and California Class Members' Private Information).

82. In violation of Cal. Civ. Code § 56.101(b)(1)(B), Keenan's electronic health record system or electronic medical record system failed to record the identity of persons who accessed and changed medical information, failed to record the date and time medical information was accessed, and failed to record changes that were made to medical information.

83. In violation of Cal. Civ. Code § 56.26(a) Keenan, as an entity engaged in the business of furnishing administrative services to health care providers or their affiliates, knowingly used, disclosed, or permitted its employees or agents to use or disclose medical information possessed in connection with performing administrative functions for a program, in a manner not reasonably necessary in connection with the administration or maintenance of the program, or in a manner not required by law, or without authorization. This violation resulted from the affirmative actions of Keenan or its agents who exposed two file servers containing Private Information on the public internet. This disclosure was an affirmative communicative act by Keenan and a violation of Cal. Civ. Code § 56.26(a). Plaintiff's and California Class Members' Private Information was viewed by

unauthorized individuals as a direct and proximate result of Keenan's violation of § 56.26(a).

84. In violation of Cal. Civ. Code § 56.36(b), Keenan negligently released confidential information or records concerning Plaintiff Rutledge and California Class Members. This negligent release of Plaintiff Rutledge's and California Class Members' Private Information to unauthorized individuals in the Data Breach resulted from the affirmative actions of Keenan or its agents who exposed two file servers containing Private Information on the public internet. This disclosure was an affirmative act by Keenan and a violation of Cal. Civ. Code § 56.36(b). Plaintiff Rutledge's and California Class Members' Private Information was viewed by unauthorized individuals as a direct and proximate result of Keenan's violation of Cal. Civ. Code § 36.36(b).

85. In violation of Cal. Civ. Code § 56.10(d), Keenan intentionally shared, sold, used for marketing, or otherwise used Plaintiff's and California Class Members' Private Information for a purpose not necessary to provide health services to Plaintiff or California Class Members.

86. In violation of Cal. Civ. Code § 56.10(e), Keenan further disclosed Plaintiff's and California Class Members' Private Information to persons or entities not engaged in providing direct health care services to Plaintiff's or California Class Members or their providers of health care service plans or insurers or self-insured employers.

87. All of Keenan's acts described herein were done knowingly and willfully by Keenan.

88. Plaintiff and California Class Members were injured and have suffered damages, as described herein, from Keenan's illegal disclosure and negligent release of their Private Information in violation of Cal. Civ. Code §§ 56.10, 56.101, 56.26 and 56.36 and therefore seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorneys' fees, expenses and costs.

89. As a direct and proximate result of Keenan's violations of the CMIA, Plaintiff and California Class Members have faced and will face an increased risk of future harm.

90. As a direct and proximate result of Keenan's violations of the CMIA, Plaintiff and California Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

91. Plaintiff and California Class Members suffered a privacy injury by having their sensitive medical information disclosed, irrespective of whether or not they subsequently suffered identity fraud, or incurred any mitigation damages. Medical information has been recognized as private sensitive information in common law and federal and state statutory schemes and the disclosure of such information resulted in cognizable injury to Plaintiff and California Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, pray for judgment as follows:

a. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class;

b. For equitable relief enjoining Keenan from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII and PHI;

c. For equitable relief compelling Keenan to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;

d. For an order requiring Keenan to pay for credit monitoring services for Plaintiff and the Class of a duration to be determined at trial;

e. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

f. For an award of punitive damages, as allowable by law;

g. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h. Pre and post-judgment interest on any amounts awarded; and

i. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: February 2, 2024

Respectfully submitted by:

By: */s/ Jonathan Shub*

Jonathan Shub (No. 237708)
Benjamin F. Johns*
Samantha E. Holbrook*
SHUB & JOHNS LLC
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
(610) 477-8380
jshub@shublawyers.com
bjohns@shublawyers.com
sholbrook@shublawyers.com

Attorneys for Plaintiff and the Proposed Class

**Pro Hac Vice Forthcoming*